THAT WHICH IS CLAIMED IS:

1. A random signal generator of the kind that uses an electronic noise source:

characterized in that the electronic noise source comprises a folded MOS transistor whose drain-source current has a random component, the generator comprising means for generating a random binary signal from the random component.

2. A generator according to claim 1, wherein the folded MOS transistor comprises an S- or zigzag-shaped channel, the size of which is at the resolution limit imposed by the transistor manufacturing technology.

3. A generator according to any of claims 1 and 2, comprising a reference transistor, to which are applied a gate voltage and a bias current that are the same as those applied to the folded transistor, for extracting the random component.

4. A generator according to any of claims 1 to 3, comprising means for comparing the random component to a detection current.

5. A generator according to any of claims 1 to 4, comprising means for amplifying the random component.

6. A generator according to any of claims 1 to 5, comprising means for sampling the random binary signal in order to obtain a random digital signal.

7. A generator according to claim 6, comprising a logic circuit (5) for generating random binary numbers from the random digital signal.

8. A generator according to any of claims 1 to 7, comprising means for automatically maintaining the gate voltage (V_G) of the folded transistor within a predetermined range of values that ensures the delivery of an equiprobable output signal.

9. A generator according to any of claims 1 to 8, comprising a plurality of electronic noise sources, which generate a current including a random component, each source being coupled, respectively, to means for generating a random binary signal from the random component generated by the source, the generator further comprising means for combining the random binary signals delivered by the sources for generating random binary signals.

10. An integrated circuit, characterized in that it comprises a random binary signal generator according to any of claims 1 to 9, and means for coupling the generator output to other components in the integrated circuit.

11. An integrated circuit according to claim 10, arranged on a support for forming a smart card or any other equivalent portable electronic item.

12. An integrated circuit according to claim 10 or 11, comprising a processor unit including means for receiving a random number generated by the generator, means for sending this random number to an external terminal, means for subjecting this random number to a secret key authentication function, means for comparing the result of this function to a result provided by the terminal in response to the random number being sent, and means for authorizing a transaction with the terminal if the result provided by

the terminal matches with a result computed by the processor unit.

13. A method for generating a random number from an electronic noise source, characterized in that it comprises the steps of:

- providing a folded transistor having an S- or zigzag-shaped channel whose size is chosen to be at the resolution limits allowed by the transistor manufacturing technology;
- extracting a random current component across the terminals of a folded MOS transistor;
- generating a binary signal as a function of the random component; and
- sampling the binary signal.

14. A method according to claim 13, comprising the steps of amplifying the random component and subtract therefrom a reference value before converting it into a binary signal.

15. A method according to any of claims 13 and 14, comprising the step of adjusting the gate voltage of the folded transistor as a function of the random binary signal obtained after the sampling step.

16. A method according to any of claims 13 and 15, comprising the step of generating binary numbers from the binary signal.